stewart
NATIONAL
COMMERCIAL SERVICES

Wire Fraud Risk Mitigation and the Security of the Commercial Closing Process

Title Tenets Webinar Series

Presented By: Megan Toborg

Wednesday, June 22, 2022

Wire Fraud Risk Mitigation and the Security of the Commercial Closing Process

In this session we will be discussing the "Who", "What", "When", "Where", and "Why" of the risks associated with the Commercial Closing Process

Who? There are two – who needs protecting and who they need protection from

What? Wire fraud and internet crime

When? Whenever we let our guard down

Where? Everywhere

Why? Money, money, money

Annual Fedwire Funds Service Statistics

According to the Federal Reserve, in **1987** the total number of wire transfers was **52,375,438** with an average wire amount of **$2,910,000**.

In **2021**, there were over **204 million** wire transfers with an average wire amount of **$4,850,000**.

That adds up to almost a quadrillion dollars sent through the United States Federal Reserve System.

QUADRILLION!!

Source: https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/annual-stats.html

Annual Fedwire Funds Service Statistics

Look at the top line of this chart.

This is what a

QUADRILLION

looks like

Year	Transfers originated (number)	Annual volume growth (percent)	Value of transfers originated[1] ($millions)	Annual value growth (percent)	Average value per transfer ($millions)	Average daily volume of transfers[2] (number)	Average daily value of transfers[2] ($millions)
2021	204,490,893	11.1	991,810,545	18.0	4.85	811,472	3,935,756
2020	184,010,202	9.8	840,483,038	20.8	4.57	727,313	3,322,067
2019	167,650,062	5.8	695,835,129	(2.8)	4.15	667,929	2,772,252
2018	158,430,742	3.8	716,211,759	(3.2)	4.52	631,198	2,853,433
2017	152,649,633	3.0	740,096,838	(3.5)	4.85	608,166	2,948,593
2016	148,142,402	3.8	766,961,537	(8.1)	5.18	590,209	3,055,624
2015	142,757,101	5.7	834,630,440	(5.6)	5.85	566,496	3,312,026
2014	135,022,749	0.6	884,551,876	24.0	6.55	537,939	3,524,111
2013	134,244,177	2.0	713,310,354	19.0	5.31	534,837	2,841,874
2012	131,637,349	3.6	599,200,625	(9.7)	4.55	524,452	2,387,253
2011	127,022,420	1.5	663,837,575	9.1	5.23	506,065	2,644,771
2010	125,130,561	0.3	608,325,851	(3.6)	4.86	496,550	2,413,991
2009	124,731,244	(5.0)	631,127,108	(16.4)	5.06	494,965	2,504,473
2008	131,362,107	(2.5)	754,974,633	12.6	5.75	521,278	2,995,931
2007	134,688,381	0.8	670,665,569	17.1	4.98	536,607	2,671,974
2006	133,605,267	0.9	572,645,790	10.4	4.29	532,292	2,281,457
2005	132,437,838	5.9	518,546,733	8.3	3.92	527,841	2,065,923
2004	125,103,104	1.5	478,946,947	7.1	3.83	494,479	1,893,071
2003	123,280,721	7.2	447,341,692	10.2	3.63	491,158	1,782,238
2002	114,979,176	2.2	405,761,750	(4.2)	3.53	458,084	1,616,581
2001	112,455,615	3.8	423,606,365	11.5	3.77	448,030	1,687,675
2000	108,313,521	5.4	379,756,389	10.6	3.51	429,816	1,506,970
1999	102,797,106	4.8	343,381,658	4.6	3.34	407,925	1,362,626
1998	98,095,841	9.6	328,748,912	14.0	3.35	389,269	1,304,559
1997	89,510,261	8.4	288,419,808	15.8	3.22	356,615	1,149,083

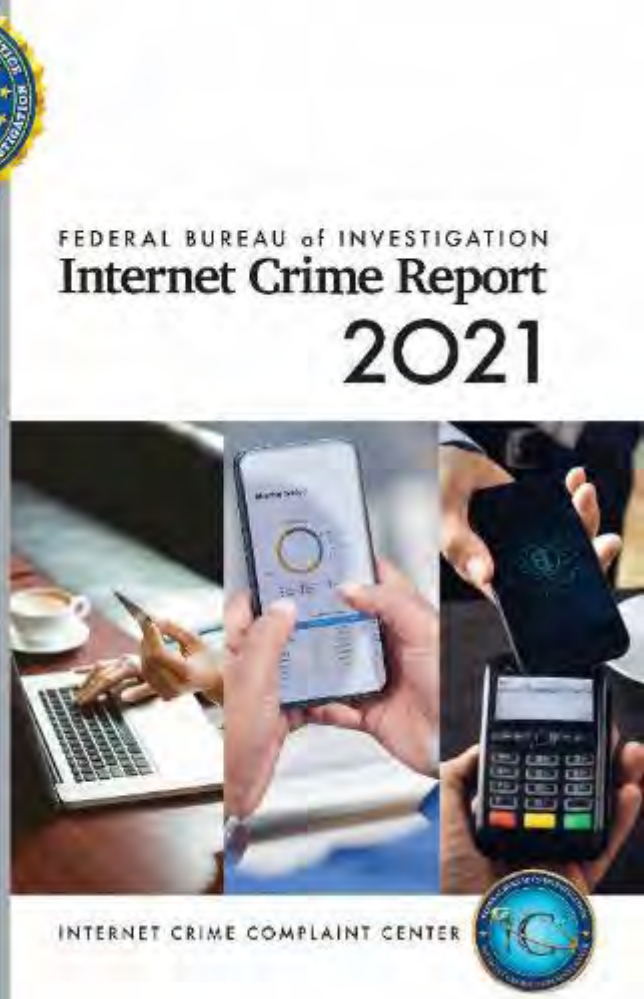
stewart NATIONAL COMMERCIAL SERVICES

Source: https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/annual-stats.html

Cybercrime

FBI Internet Crime Report

Cybercrime has become so prevalent that the FBI issues an Internet Crime Report to track it.



Source: https://www.ic3.gov/

stewart
NATIONAL
COMMERCIAL SERVICES

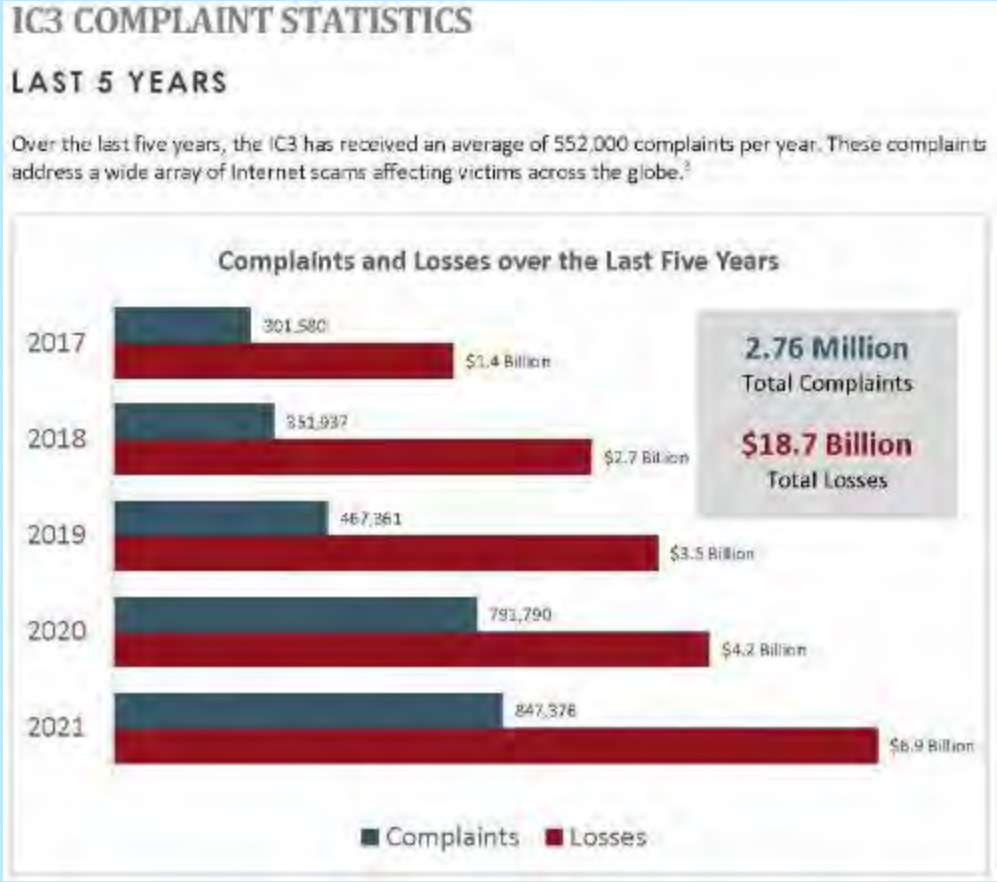
Cybercrime

FBI Internet Crime Report

In 2021, there were losses due to internet crime exceeding $6.9 billion.

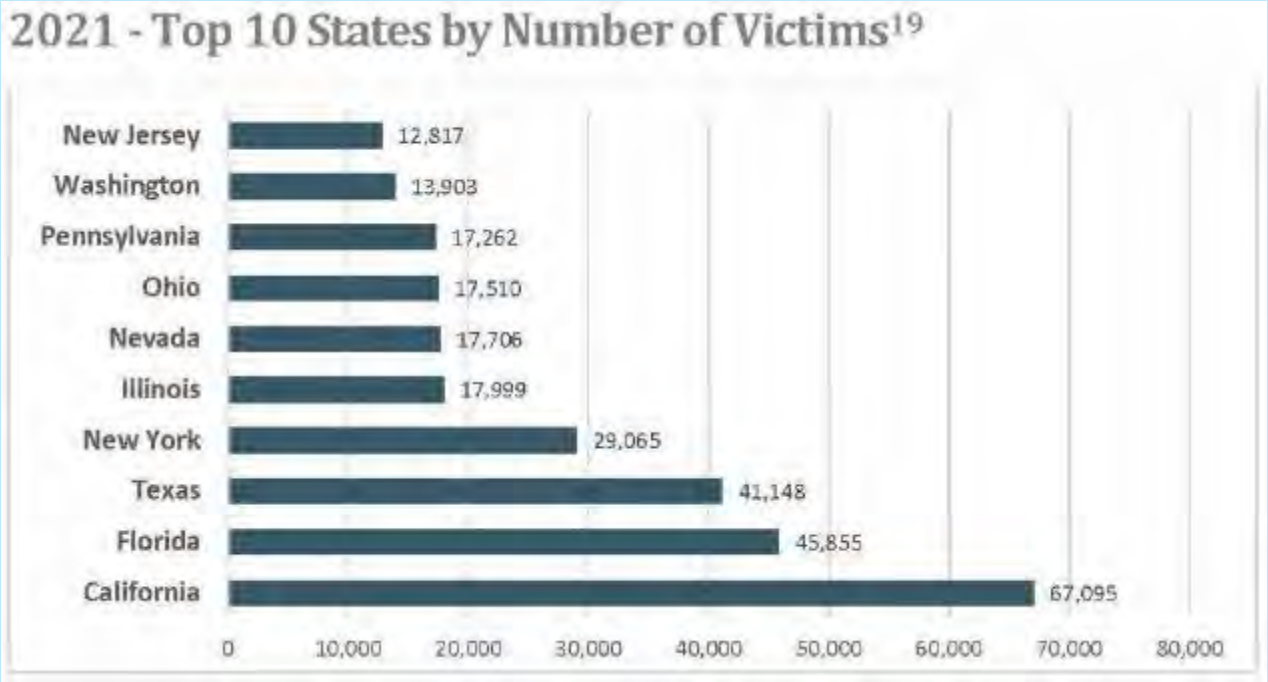
In 2017, that number was $1.4 billion.

THAT IS A HUGE JUMP IN CYBERCRIME IN JUST 5 YEARS!



Source: https://www.ic3.gov/

See where the criminals have been especially busy



Source: https://www.ic3.gov/

Nevada is out; Michigan is in – worst March Madness bracket ever

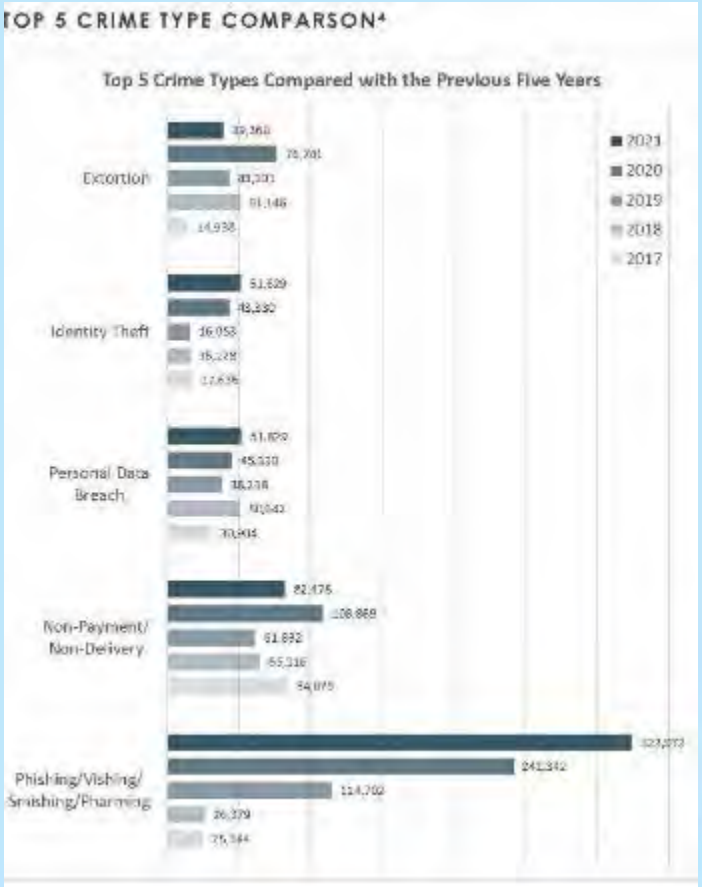
Source: https://www.ic3.gov/

What Cybercrimes are the most prevalent?

In 2017, there were a little over 25,000 reported cases of Phishing / Vishing / Smishing / Pharming.

In 2021 there were over 300,000 reported cases.

Be afraid, be very afraid.



Source: https://www.ic3.gov/

Title Tenets Webinar Series

What are Phishing, Vishing, and Smishing???

And does changing the font make them less dangerous?
Spoiler Alert - NO

PHISHING

VISHING

SMISHING

Phishing

Vishing

SMISHING

Phishing

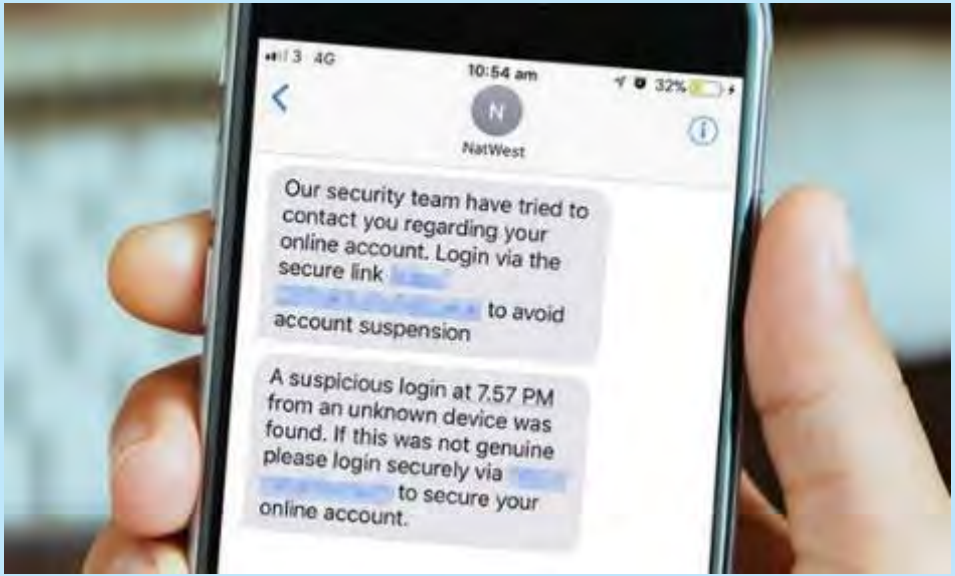
Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as a password or credit card numbers.

Vishing

Vishing is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

Smishing

Smishing is the fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.



I guess this is about fraud, huh?

Clearly, the definitions are all basically the same but for the technology used, but what does it all really mean??

Storytime

Story 1 - Phishing

In an article by ABC7 Chicago, in 2021, Jenna Carlson was ready to put down her life savings on her dream home. The deposit amount was $42,000 and the paralegal for the law firm helping her with the transaction said she would send her wire instructions the following week. The same day, though, Jenna received an email from the paralegal indicating the money needed to be deposited sooner. Wire instructions were attached along with the correct amount, correct property address, and correct mortgage commitment document. She went back and forth with the “paralegal” via email clarifying information and then headed to her bank where she had a wire transfer initiated. The following week, the paralegal called about the down payment and that is when Jenna realized something was wrong. She looked more closely at the email and saw that there were extra letters in the email address that she hadn’t noticed. Someone had gone Phishing and by the time the fraud was realized, Jenna’s money was gone.

Source: https://abc7chicago.com/house-down-payment-wire-transfer-instructions-fraud-mortgage/11670854/

Lesson 1

Something experts always caution against is acting on urgent directives. Since Jenna had been told it wouldn't be until the following week, when she received the wire instructions with direction to wire transfer the funds sooner, she should have stopped dead in her tracks. Jenna also carried out all her conversations via email rather than making a phone call and verbally verifying the directions. In addition, she didn't follow up to confirm receipt of her wire.

Biggest takeaways - Unexpected communication with a sense of urgency should ALWAYS be a red flag and make sure to follow up.

Story 2 - Vishing

In early 2019, a Vishing scam that used AI to mimic the voice and intonation of a German executive was convincing enough to be successful. The man receiving the call was told he needed to wire funds within the hour. Although this was not a normal request, this man, thinking he was following the verbal orders of his boss, sent the funds in the amount of $243,000. The scammers called later trying to get another wire sent but by then the man had become suspicious. Unfortunately, it was too late as the initial wire had been received by the scammers and quickly moved to a different bank in a different country.

Source: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Lesson 2

This is a tough one. Most people would think a familiar voice should be safe. Whether you think you recognize the voice or not, if you're being asked unexpectedly to do something outside the normal course of business, even if it is a familiar voice, you should definitely take some steps to make sure nothing is amiss.

Story 3 - Vishing

Forbes reported in 2020 that there was a data breach at the Ritz Carlton in London that evolved into Vishing attacks. The messages were highly targeted and purported to be from the hotel itself. The scammers went so far as to spoof the hotel's actual phone number and called guests requesting credit card information. The guests, who believed they were speaking to a Ritz representative, handed over their information and, with it, access to their accounts.

Source: https://www.forbes.com/sites/emilsayegh/2020/09/30/vishing-at-the-ritz-theres-a-new-type-of-cybercrime-in-town/?sh=27e16078700d

Lesson 3

This is another example of scammers preying on people's natural instincts to not question a request from someone who seems to know what they're talking about. By now, you've probably seen more than one message from your credit card company or your bank stating that they will never solicit identifying information through email or text. Some messages go so far as to remind you that they will never call you to get your PIN. There's a reason for these messages.

There is no legitimate reason that someone would call you and ask for your account number, credit card number, or PIN.

Story 4 - Smishing

Smishing, the term coming from “SMS” or short message service, is similar to Phishing but is an attack using text messaging. You’ve probably gotten a text with a link to track an Amazon package when you hadn’t ordered anything or from a bank saying there was an issue with your account. Hopefully, you’ve deleted the text messages, or you could end up like one of the people who were scammed by three Romanian men who compromised computers between 2011 and 2014, initiating thousands of phone calls and text messages that tricked people into disclosing personal information, including account numbers and social security numbers. When caught, between the three men they had over 40,000 account numbers and had defrauded people in excess of $21,000,000.

Source: https://www.aarp.org/money/scams-fraud/info-2020/smishing.html

Source: https://arstechnica.com/information-technology/2019/03/3-men-plead-guilty-to-vishing-and-smishing-scheme-estimated-to-cost-21-million/

Lesson 4

It would seem obvious but never, ever, ever reply to an unsolicited text message with private information.

DELETE. DELETE. DELETE. (But remember, if we've learned anything from shows like NCIS, it's that nothing is ever really deleted, but at least it will keep you from clicking on a link or responding by accident)

Whether it is a text or a Facebook message or a notice on What'sApp, no one that can be trusted would be asking for this information.

Story 5 - Phishing

Real estate attorneys, brokers, and title companies are some of the hardest hit when it comes to Phishing attacks. Cybercriminals hack into their computer system and snoop around, finding details on upcoming closings. They then send legitimate sounding and looking emails to the homebuyer with fraudulent wire instructions directing them to send funds. Often, by the time anyone realizes what happened, the money is long gone. To dissuade anyone of the notion that a highly educated person cannot fall victim to something like this, take, for example, the story of former NY State Supreme Court Justice Lori Sattler. She received an email from her attorney. At least that's what she thought. She was directed to wire $1,057,000 for her "closing". She followed instructions and her funds ended up at a bank in China rather than with the settlement agent.

Source: https://www.law.com/njlawjournal/2022/01/19/lawyers-title-insurance-companies-targeted-in-one-of-the-hottest-real-estate-scams/?slreturn=20220516160957

Lesson 5

No one is immune to these kinds of attacks. NO ONE.

The scammers prey on everyone. Nothing protects you from being a target.

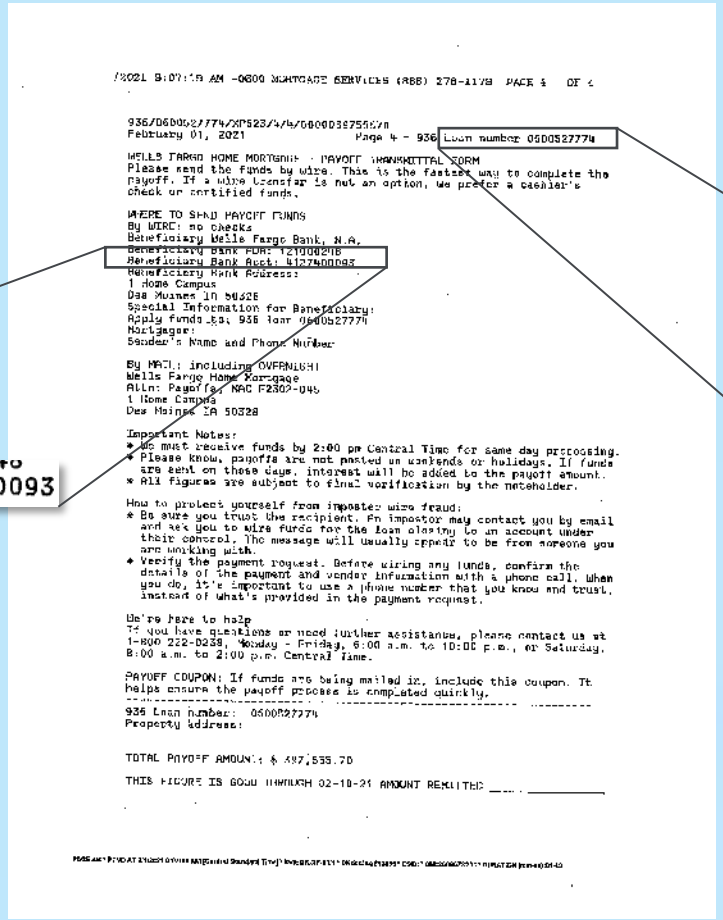
What IS wire fraud?

Office of the Law Revision Counsel
UNITED STATES CODE

18 U.S. Code Section 1343

Wire fraud is defined as recklessly and intentionally making a material misrepresentation to deprive another person of something that has value.

Source: https://uscode.house.gov/



/2021 8:07:19 AM -0600 MORTGAGE SERVICES (RBB) 278-1178 PAGE 4 OF 4

936/0600527774/XP523/4/4/0600D3875570
February 01, 2021 Page 4 - 936 Loan number 0600527774

WELLS FARGO HOME MORTGAGE - PAYOFF TRANSMITTAL FORM
Please send the funds by wire. This is the fastest way to complete the payoff. If a wire transfer is not an option, we prefer a cashier's check or certified funds.

WHERE TO SEND PAYOFF FUNDS
By WIRE: no checks
Beneficiary Wells Fargo Bank, N.A.
Beneficiary Bank FDA: 121000248
Beneficiary Bank Acct: 4127400093
Beneficiary Bank Address:
1 Home Campus
Des Moines IA 50328
Special Information for Beneficiary:
Apply funds for: 936 loan 0600527774
Mortgagor:
Sender's Name and Phone Number

By MAIL: including OVERNIGHT
Wells Fargo Home Mortgage
Attn: Payoffs, MAC F2302-045
1 Home Campus
Des Moines IA 50328

Important Notes:
* We must receive funds by 2:00 pm Central Time for same day processing.
* Please know, payoffs are not posted on weekends or holidays. If funds are sent on these days, interest will be added to the payoff amount.
* All figures are subject to final verification by the noteholder.

How to protect yourself from imposter wire fraud:
* Be sure you trust the recipient. An impostor may contact you by email and ask you to wire funds for the loan closing to an account under their control. The message will usually appear to be from someone you are working with.
* Verify the payment request. Before wiring any funds, confirm the details of the payment and vendor information with a phone call. When you do, it's important to use a phone number that you know and trust, instead of what's provided in the payment request.

We're here to help
If you have questions or need further assistance, please contact us at 1-800 222-0238, Monday - Friday, 6:00 a.m. to 10:00 p.m., or Saturday, 8:00 a.m. to 2:00 p.m. Central Time.

PAYOFF COUPON: If funds are being mailed in, include this coupon. It helps ensure the payoff process is completed quickly.

936 Loan number: 0600527774
Property address:

TOTAL PAYOFF AMOUNT: $ 497,535.70

THIS FIGURE IS GOOD THROUGH 02-10-21 AMOUNT REQUIRED _____

Beneficiary Bank Acct: 4127400093

Loan number 0600527774

02/01/2021 3:07:19 AM -0500 MORTGAGE SERVICES (866) 278-1178 PAGE 4 OF 4

936/06005277774/XP523/4/5/0000039/000/0

February 01, 2021 Page 4 - 936 Loan number 06005277774

WELLS FARGO HOME MORTGAGE - PAYOFF TRANSMITTAL FORM
Please send the funds by wire. This is the fastest way to complete the payoff. If a wire transfer is not an option, we prefer a cashier's check or certified funds.

WHERE TO SEND PAYOFF FUNDS
By WIRE: no checks
Beneficiary Wells Fargo Bank, N.A.
~~Beneficiary Bank ABA: 121000248~~
Beneficiary Bank Acct: 41274000093
Beneficiary Bank Address:
1 Home Campus
Des Moines IA 50328
Special Information for Beneficiary:
Apply funds to: 936 loan 06005277774
Mortgagor:
Sender's Name and Phone Number

By MAIL: including OVERNIGHT
Wells Fargo Home Mortgage
Attn: Payoffs, MAC F2302-045
1 Home Campus
Des Moines IA 50328

Important Notes:
* We must receive funds by 2:00 pm Central Time for same day processing.
* Please know, payoffs are not posted on weekends or holidays. If funds are sent on those days, interest will be added to the payoff amount.
* All figures are subject to final verification by the noteholder.

How to protect yourself from imposter wire fraud:
* Be sure you trust the recipient. An imposter may contact you by email and ask you to wire funds for the loan closing to an account under their control. The message will usually appear to be from someone you are working with.
* Verify the payment request. Before wiring any funds, confirm the details of the payment and vendor information with a phone call. When you do, it's important to use a phone number that you know and trust, instead of what's provided in the payment request.

We're here to help
If you have questions or need further assistance, please contact us at 1-800-222-0258, Monday - Friday, 6:00 a.m. to 10:00 p.m., or Saturday, 8:00 a.m. to 2:00 p.m. Central Time.

PAYOFF COUPON: If funds are being mailed in, include this coupon. It helps ensure the payoff process is completed quickly.

936 Loan number: 06005277774
Property address:

TOTAL PAYOFF AMOUNT: $ 397,555.70

THIS FIGURE IS GOOD THROUGH 02 10-21 AMOUNT REMITTED _____

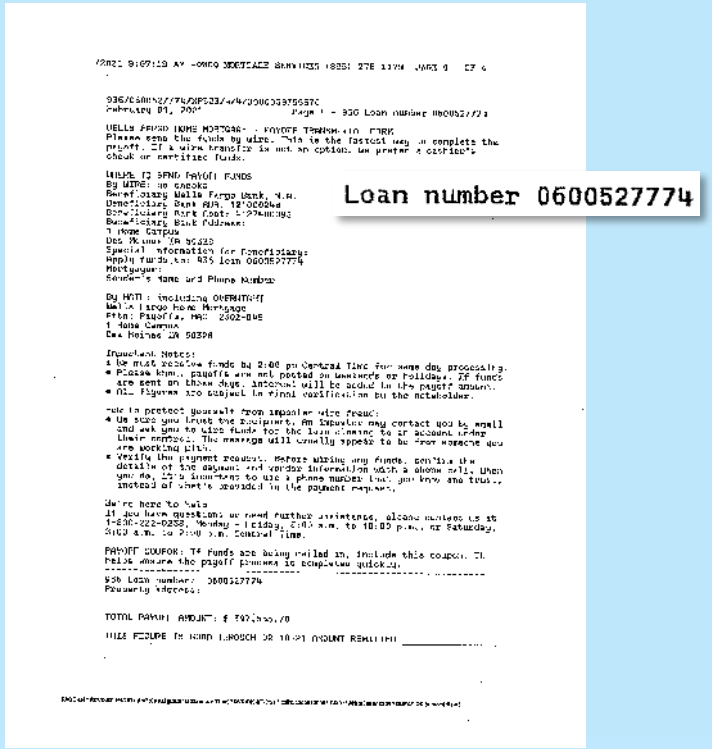
Beneficiary Bank ABA: 121000248
Beneficiary Bank Acct: 41274000093

Loan number 06005277774

Side by Side Comparison of wire instructions

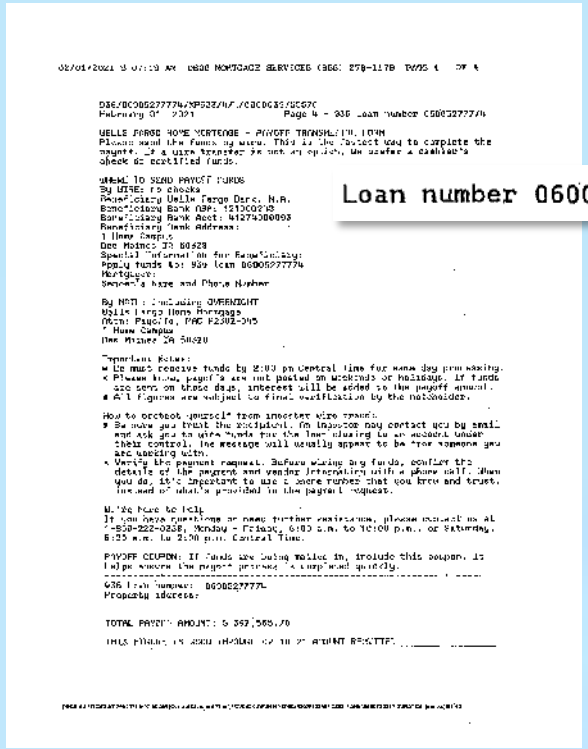
Beneficiary Bank Acct: 4127400093

Loan number 0600527774



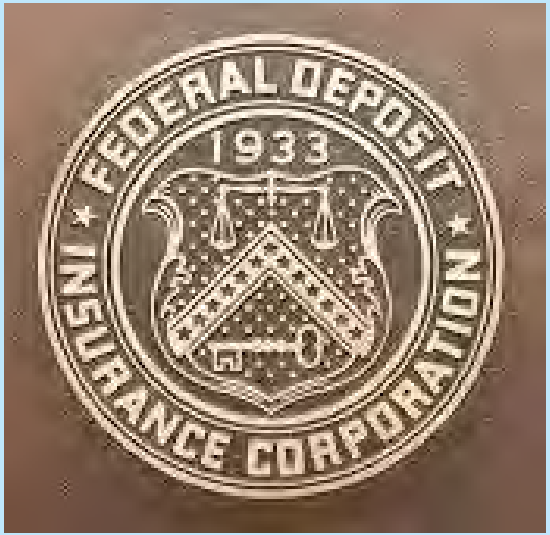
Beneficiary Bank Acct: 41274000093

Loan number 06005277774



Title Tenets Webinar Series

FBI, FDIC, FinCEN



What can you do?

We can't rely only on government agencies to protect us. We must protect ourselves.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2022

Alert Number
I-050422-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Business Email Compromise: The $43 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-091019-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2021.

Source: https://www.ic3.gov/Media/Y2022/PSA220504

Definition of BEC

Business Email Compromise is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests. The scam is typically done through social engineering or computer intrusion.

It is not always associated with a transfer-of-funds request. One type of BEC requests employees' W-2 forms to gather personal information.

Who gets hit?

FBI's Six Types of BEC Fraud

A CEO directs an accounting staff member to send funds to another party

A supplier asking for their payment to be sent to a new address or bank account

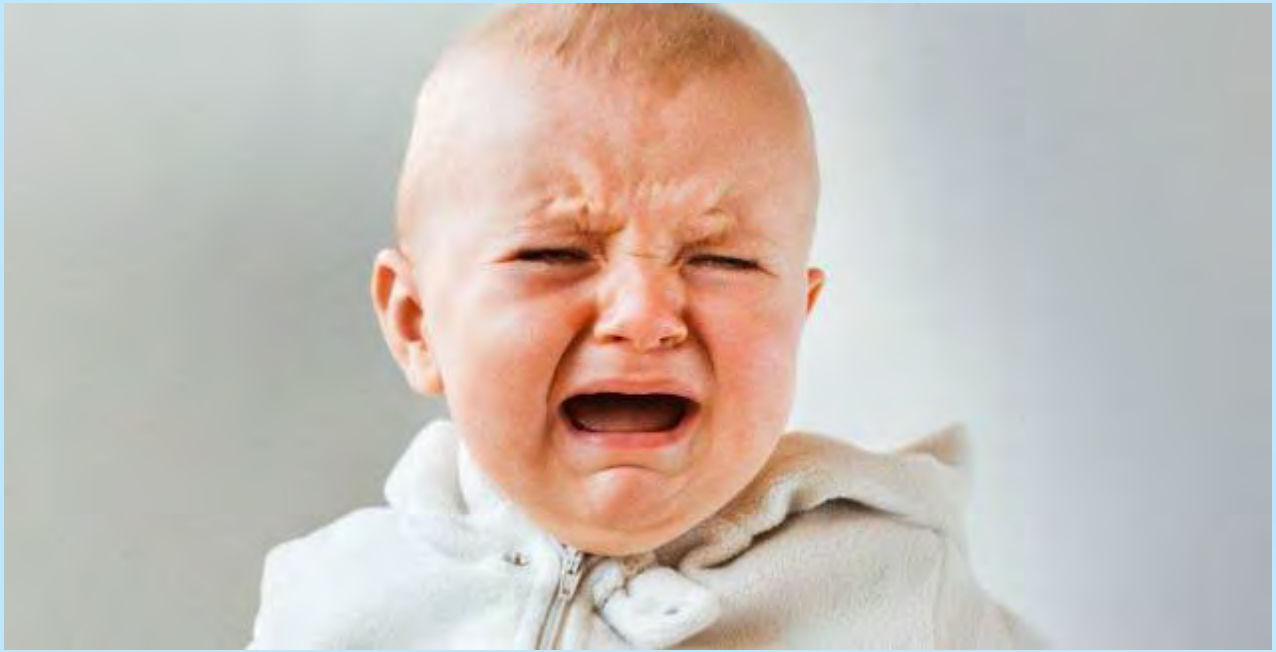
An executive requests copies of employees W-2 forms

A real estate professional diverting escrow payment, deposits, or proceeds to a new account

A direct deposit change from an employee

A clergyman or employer asking for donations for their organization

Hopes Dashed



BEC Statistics

The following BEC/EAC statistics were reported to the FBI IC3, law enforcement and derived from filings with financial institutions between **June 2016 and December 2021**:

Domestic and international incidents:	**241,206**
Domestic and international exposed dollar loss:	**$43,312,749,946**

The following BEC/EAC statistics were reported in victim complaints to the IC3 between **October 2013 and December 2021:**

Total U.S. victims:	**116,401**
Total U.S. exposed dollar loss:	**$14,762,978,290**
Total non-U.S. victims:	**5,260**
Total non-U.S. exposed dollar loss:	**$1,277,131,099**

The following statistics were reported in victim complaints to the IC3 between **June 2016 and December 2021:**

Total U.S. financial recipients:	**59,324**
Total U.S. financial recipient exposed dollar loss:	**$9,153,274,323**
Total non-U.S. financial recipients:	**19,731**
Total non-U.S. financial recipient exposed dollar loss:	**$7,859,268,158**

Source: https://www.ic3.gov/Media/Y2022/PSA220504

Where to start

VIGILANCE

The simplest thing you can do is pay attention to what you're doing. Awareness is key.

RED FLAGS

Be on the lookout for warning signs and things that just don't seem right

ACT FAST

If you ARE a victim of wire fraud, don't be embarrassed and don't delay.

Vigilance

- Strong passwords
- Consistent procedures
- Anti-virus software
- Avoid “the click”
- Encryption
- Get personal

Strong Passwords

Do not use sequential numbers or letters

Do not include your birth year, month, or day

Use a combination of at least 8 letters, numbers, and symbols

Combine words and numbers into phrases, if the words are unrelated even better

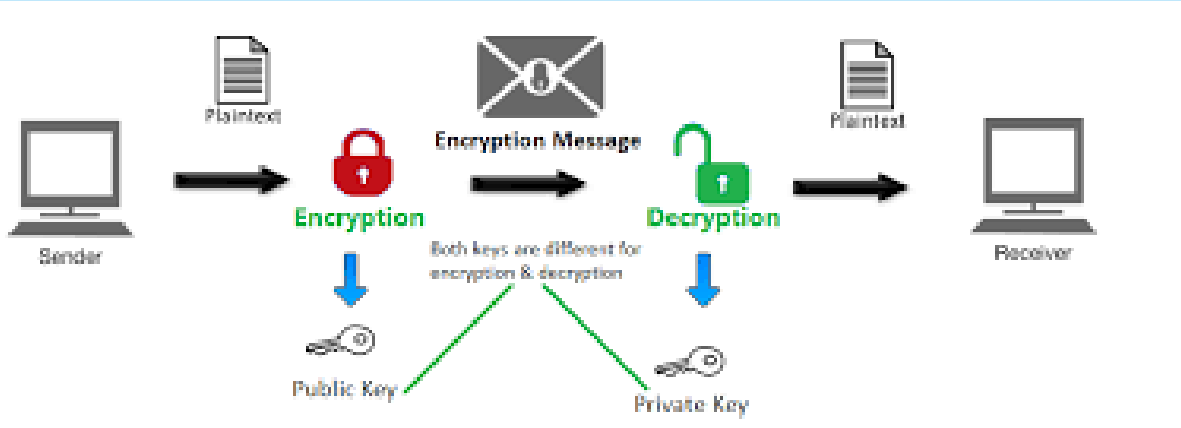
Do not use names of family members or colleagues

Do not reuse passwords or use the same password for more than one login

Do not share passwords

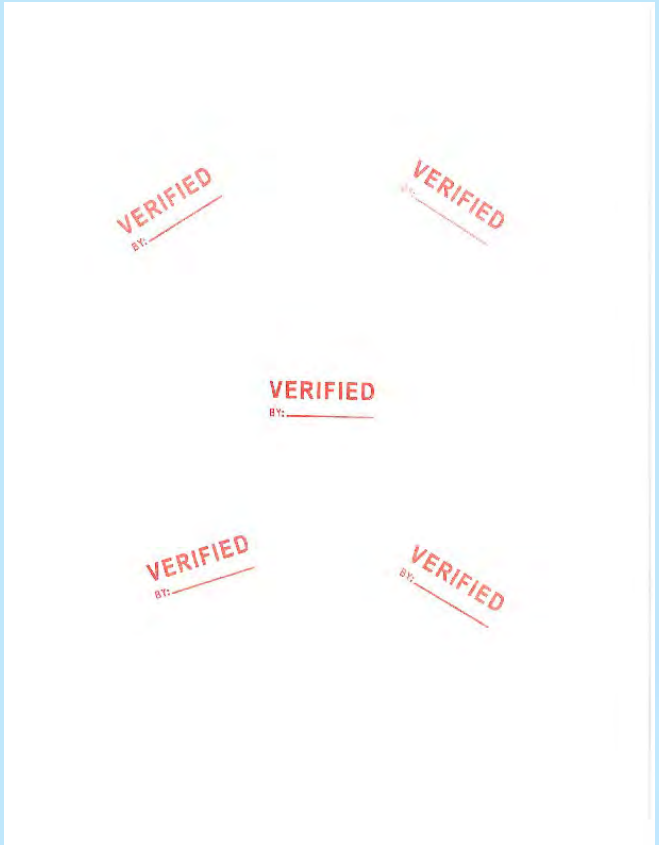
Antivirus Software

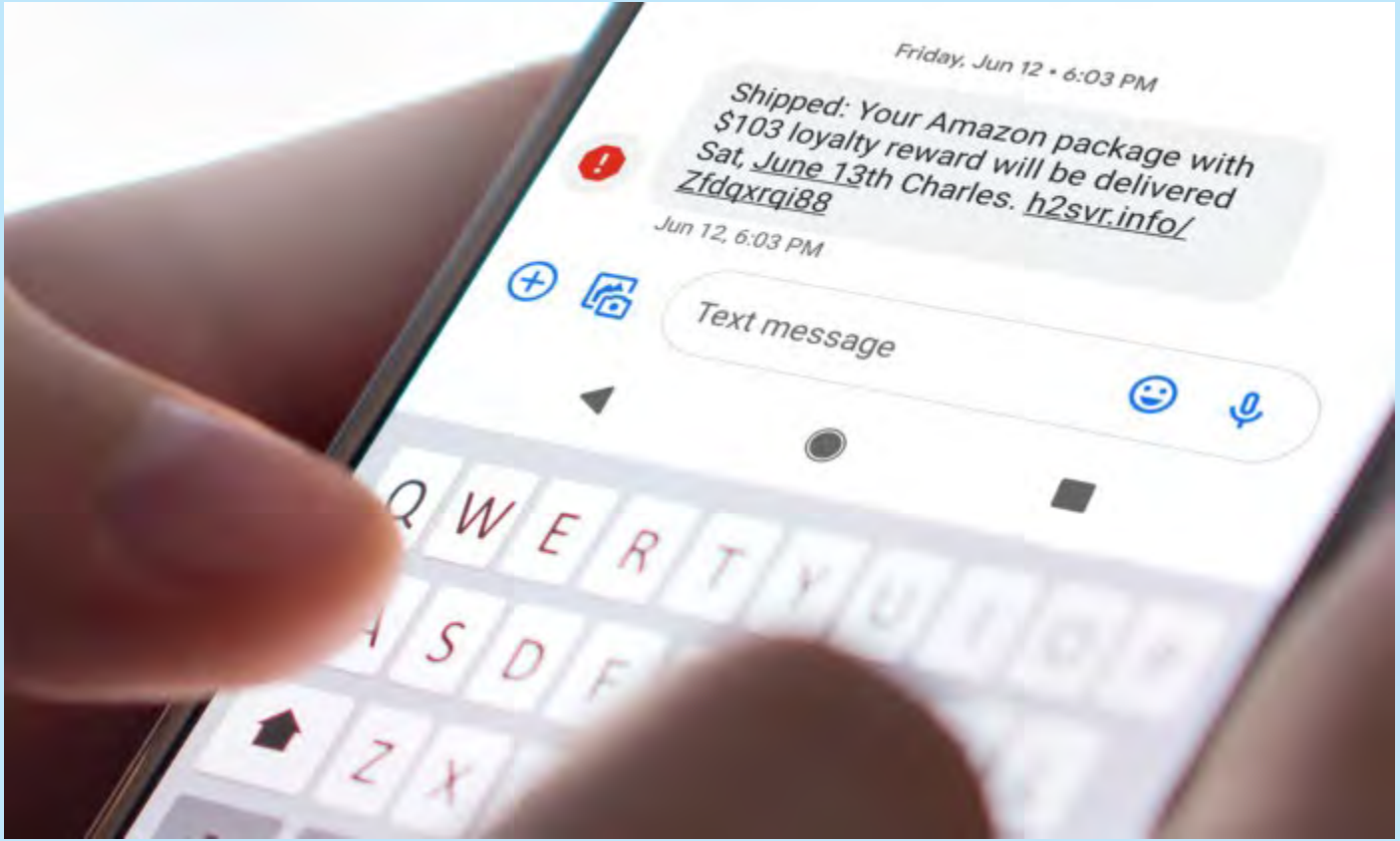
Encryption



Verify, verify, verify

As an example, part of our procedure requires that every wire that my office sends out has a “Verified” stamp on it. The person in our office who verbally verified the instructions must stamp the instructions, put their initials and the date verified, and below the stamp write the name of the person they spoke with and their phone number. If there is no “Verified” stamp, then the wire does not get approved and released. No deviation from this is allowed. Period.





Red Flags

Examples of Red Flags

You receive an email with wire instructions from an attorney. Shortly thereafter you receive a follow up email with new wire instructions. Assume they are not legitimate.

We live in a fast-paced world, and everything seems like it needs to happen now, now, NOW. But does it? There is a life cycle to the closing process. Know where you are in that process.

Poor grammar and spelling errors besides the invariable “Your welcome” or “there” instead of “their”.

ACT FAST

BEC Statistics – Redux

The following BEC/EAC statistics were reported to the FBI IC3, law enforcement and derived from filings with financial institutions between **June 2016 and December 2021**:

Domestic and international incidents:	**241,206**
Domestic and international exposed dollar loss:	**$43,312,749,946**

The following BEC/EAC statistics were reported in victim complaints to the IC3 between **October 2013 and December 2021:**

Total U.S. victims:	**116,401**
Total U.S. exposed dollar loss:	**$14,762,978,290**
Total non-U.S. victims:	**5,260**
Total non-U.S. exposed dollar loss:	**$1,277,131,099**

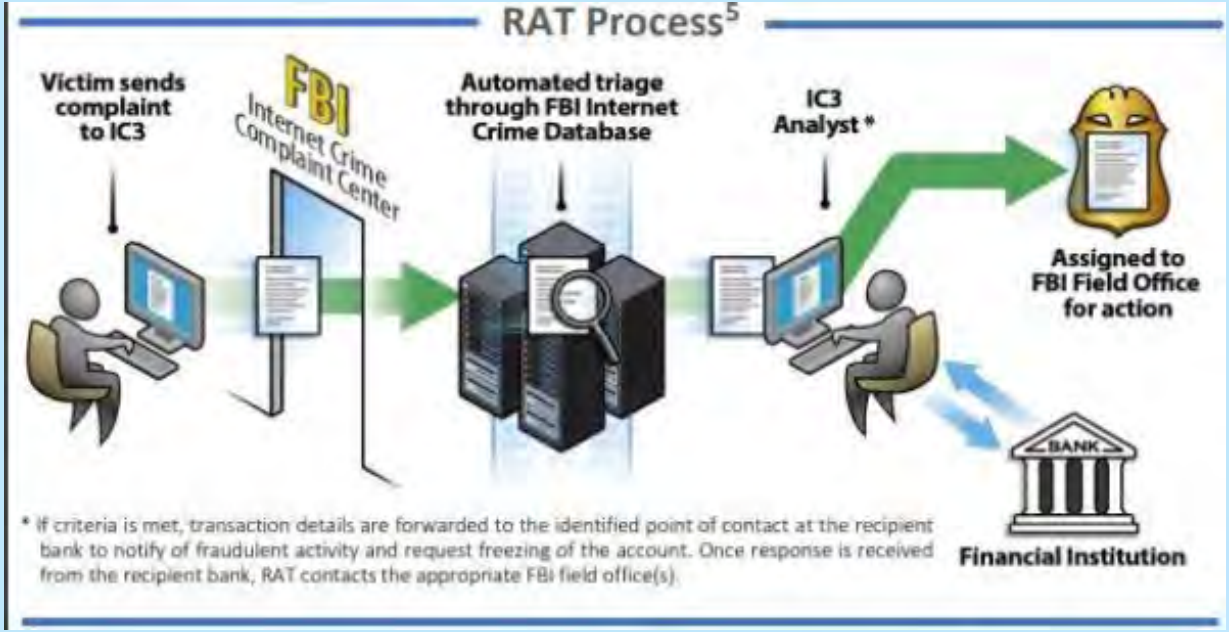
The following statistics were reported in victim complaints to the IC3 between **June 2016 and December 2021:**

Total U.S. financial recipients:	**59,324**
Total U.S. financial recipient exposed dollar loss:	**$9,153,274,323**
Total non-U.S. financial recipients:	**19,731**
Total non-U.S. financial recipient exposed dollar loss:	**$7,859,268,158**

Source: https://www.ic3.gov/Media/Y2022/PSA220504

The Internet Crime Complaint Center (IC3) Recovery Asset Team (RAT) is ready to act as soon as they are notified.

Source: https://www.ic3.gov/



Source: https://www.ic3.gov/

Philadelphia

In December 2021, the IC3 received a complaint filed by a victim regarding a wire transfer of over $1.5 million to a fraudulent U.S. domestic bank account. They notified the recipient financial institution. Coordination between the IC3 RAT, the recipient financial institution, and the Philadelphia FBI field office resulted in the knowledge that the criminal had depleted the wired funds from the original account and moved them into two separate accounts at the same institution. The financial institution was able to identify the second accounts and freeze the funds.

Source: https://www.ic3.gov/

Memphis

In June 2021, the IC3 received a complaint from a law office regarding a wire transfer of almost $200,000 to a fraudulent account. IC3 RAT working with the Memphis FBI Field Office and the recipient financial institution found that the domestic account had a corresponding fraudulent account in Nigeria. They contacted international partners and were able to freeze the full amount.

Source: https://www.ic3.gov/

Storytime

Just last week, one of our closers had a situation where fast action meant all the difference. They had followed all the procedures we have in place. The buyer too was vigilant and called the closer to verbally verify the wire instructions they received were correct. They were. The buyer wired the funds and the closer confirmed receipt. There was another party, though, that was apparently wiring funds and they received them from the broker who had received them from the buyer. Unfortunately, somewhere between the buyer, the broker, and the party sending the wire, a cybercriminal snuck in. More unfortunate, the party sending the wire did NOT call to verify the instructions. Because of hypervigilance, my closer provided regular updates to the parties and let them know that the funds had not been received. The closer asked to see what wire instructions were used and quickly realized fraud had taken place. She notified her manager and the accounting department. The accounting department notified the bank. Because fraud is so rampant, many banks have a fraud department that hold wires they suspect are not legitimate. Luckily, they had done so in this case and the funds were stopped, returned to sender, and then sent to escrow using the correct VERIFIED wire instructions.

Time to get personal

Meet and get to know your clients

Encourage kick-off video or conference calls

Gather accurate contact information at the beginning of the transaction

stewart
NATIONAL
COMMERCIAL SERVICES

Questions?

I know someone wants to ask about the chainsaw accident

Stewart Title Guaranty Company
Commercial Services
Megan Toborg
Vice President
Escrow Operations Manager
10 S. Riverside Plaza, Suite 1450
Chicago, IL 60606
312.857.7202 main
mtoborg@stewart.com
Stewart.com

Thank you

Title Tenets Webinar Series